For release on delivery
11:00 a.m. EDT (9:00 a.m. local time)
September 29, 2026

Opening Remarks

by

Michelle W. Bowman

Vice Chair for Supervision

Board of Governors of the Federal Reserve System

(via pre-recorded video)

at the

Community Bank Cyber Workshop

Denver, Colorado

September 29, 2026

Good morning, and welcome to the 2026 Community Bank Cyber Workshop.[1] It is a pleasure to join you again for this annual event hosted by the Federal Reserve Banks of Chicago, Kansas City, St. Louis, Minneapolis, and San Francisco. As the cyber environment grows more complex, events like this one enable us to continue the discussion of evolving approaches to address these challenges.

Over the past year, a number of community banks have experienced significant cyber events, which emphasizes the importance of cyber hygiene and resiliency. This workshop offers community banks practical information to help prepare for potential cyber disruptions and brings together regulators, bankers, law enforcement, and industry professionals to advance the conversation on cyber and IT risk management.

Throughout the next two days, you will gain valuable perspective through a cybersecurity tabletop exercise, explore how AI can enhance cyber defenses and its potential risks, hear from the Secret Service and the Federal Reserve's Cybersecurity Analytics Support Team, and engage more deeply with examiners, community bankers, and industry professionals, including those from the Cyber Risk Institute.

The cyber threat landscape has advanced exponentially. While banks continue to face a number of risks like ransomware, business email compromise, and vendor data breaches, the increased availability and use of AI by threat actors adds complexity to the risk environment. AI offers great potential—both to threat actors and those buttressing their defenses to those threats. It has the ability to accelerate vulnerability identification, create sophisticated social engineering campaigns, lower the barrier to entry for cyber criminals, and adapt attacks in real time as they are carried out.

---

[1] The views expressed here are my own and are not necessarily those of my colleagues on the Federal Reserve Board or the Federal Open Market Committee.

These changes have clear impacts on banks—they must continuously evolve cyber defense strategies and tactics. Defending against these risks begins with strong cyber hygiene—up-to-date asset inventories, phishing-resistant multifactor authentication, strong identity and access controls, and robust vulnerability identification and patch management programs. It also requires comprehensive employee training and periodic incident response program testing. AI is becoming a critical component of these security measures as both a defensive tool and an evolving risk.

Many of you are already exploring how to safely and strategically deploy AI for these purposes. Understanding when, where, and how to properly use AI is instrumental to balancing innovation with sound risk management. Over the summer, under my leadership of the Standing Committee on Supervisory and Regulatory Cooperation, the Financial Stability Board published a report on *Sound Practices for Responsible Adoption of AI*.[2] This report offers several practices for financial institutions to consider in the adoption and use of this technology. Some of the case studies described in the report were targeted to smaller financial institutions, and I welcome feedback from community banks about how we can continue to improve clarity for our expectations for smaller banks.

Cybersecurity requires proactive risk management by boards of directors and senior management. It also requires strategic investments in people, processes, and technology that are aligned with the risk and complexity of the institution. Regulators recognize that this can be burdensome and challenging for community banks. That's why we continue to tailor our approach to IT examinations to consider risk profile and

[2] See Financial Stability Board, *Sound Practices for Responsible Adoption of Artificial Intelligence (AI)* (FSB, June 10, 2026), https://www.fsb.org/uploads/P100626.pdf.

emerging threats and risks. This year's workshop demonstrates the Federal Reserve System's ongoing commitment to identify and equip community banks with resources that may be necessary to combat cyber risks.

In closing, cyber readiness is not built through technology alone. It requires collaboration with internal and external stakeholders, continuous education and training, and support for those on the front lines: your employees and your customers.

Thank you again to the five Reserve Banks involved in organizing this year's event. If I leave you with one thought to frame these discussions, cyber resilience is built upon a strong cyber security foundation fortified one step at a time. I hope you find that this event enhances your ability to strengthen that foundation.